Before the
Department of Transportation
Washington, D.C. 20590

In the Matter of
Privacy Act Notice Concerning Aviation Security Screening Records

DOT/TSA 010 - OST-1996-1437

Comments of the
Electronic Privacy Information Center
February 24, 2003

The Electronic Privacy Information Center (EPIC) submits these comments on the application of federal privacy rules to the collection and use of personal information obtained by the Transportation Security Administration (TSA). The TSA proposes a system of records that concerns creating a new database of Aviation Security Screening Records ("Passenger Database"), according to the Privacy Act notice published in the Federal Register on January 15, 2003.[1] According to a further notice filed the same day by the Department of Transportation (DOT), the DOT proposes to exempt this Passenger Database from certain record keeping obligations under the Privacy Act, stating that it may limit disclosures about the system because it is being used for law enforcement purposes.[2]

In summary, the TSA has failed to provide sufficient information for the public to contribute meaningfully to this rule-making procedure. In fact, the TSA has resisted requests brought under the Freedom of Information Act (FOIA) to provide public access to relevant information in the agency's possession. EPIC expressly reserves the right to

[1] Federal Register: January 15, 2003 (Volume 68, Number 10) [Page 2101-2103].
[2] Federal Register: January 15, 2003 (Volume 68, Number 10) [Page 2002].

supplement our comments after the TSA has provided further information requested below.

EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. We believe that government security proposals can and should be designed to protect privacy and other important Constitutional values. Transparency about the proposals is a critical first step for the public to evaluate the effectiveness and implications of new security measures, and public debate is crucial for the long-term viability and legitimacy of the security measures. The TSA has not provided substantive information to allow the public to properly evaluate its Passenger Database proposals, and consequently has raised serious questions about whether it is performing its public duty appropriately.

Proposed System Does Not Meet Basic Privacy Act Requirements

TSA proposes to collect passenger manifest information on all airline travelers and store it in a large centralized database. The manifest information includes "Passenger Name Records (PNR) and associated data." This includes date and time of flights, flight number, destination, reservation information, and payment information. According to the Privacy Act notice the TSA would store the records until the "completion of the individual's air travel to which the record relates."

The TSA also proposes to collect and store data on "individuals who are deemed to pose a possible risk to transportation or national security." If a person is determined to be a "risk" under this opaque (and possibly arbitrary and/or discriminatory) procedure,

the data will be stored for 50 years. The TSA, to date, has provided absolutely no information about how a passenger is determined to be a "possible risk to transportation or national security." Indeed, one could argue that simply purchasing a ticket makes an individual a "possible" risk to transportation. TSA also gives no information about how such a person might become aware of his or her categorization, and how that categorization might be legally challenged.

The TSA proposes that if a person is determined to be a risk, the database will also be populated by detailed data about that person including "risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources."

The Privacy Act requires the agency to collect data directly from the subject as far as possible, and to provide rights of access and correction.[3] However, the TSA has provided no information about where the data will be collected from, whether those sources are accurate, whether the data will be collected following lawful procedures based upon a showing of particularized suspicion, and whether the data subject will have rights of access and correction. In fact, the TSA notice explicitly denies the right provided by the Privacy Act to access the system of record for the "purposes of determining if the system contains a record pertaining to a particular individual."[4]

The Privacy Act also limits the collection of information by requiring that only relevant data be collected for a limited purpose.[5] The TSA has not provided any clarity on the actual purpose of this data collection, or whether the creation of a Passenger Database is narrowly tailored to that purpose. Furthermore, there do not appear to be any

[3] 5 U.S.C. §552(e) and (d).
[4] 5 U.S.C. §552(a)(k).
[5] 5 U.S.C. §552(e)(1).

restrictions on potential uses of the Passenger Database by other agencies of the government. The data can also be widely shared with Federal, State, local, and even international agencies.

Significantly, the TSA notice already expands the secondary purposes for the data by providing Federal, State, or local agencies access to the Passenger Database to make hiring decisions, grant licenses, and security clearances. There appears to be no limit on the possible applications for the Passenger Database information, and no restrictions on how the information might be used to make determinations.

TSA Surveillance Schemes Are Shrouded in Secrecy

There is a basic lack of public understanding about whether the proposed Passenger Database is the foundation for the Computer Assisted Passenger Pre-Screening System-II (CAPPS-II) initiative, or whether it is a repository for various government agency watch list or "no-fly" data. If indeed it forms the basis for CAPPS-II, it is very troubling that the TSA may, through this notice, be launching one of the "largest domestic surveillance systems"[6] without the opportunity for informed public debate and Congressional scrutiny. The TSA should immediately clarify its intentions regarding the purpose of the Passenger Database.

Is the Passenger Database Related to CAPPS-II?

EPIC has sought to obtain information from the TSA about CAPPS-II under the Freedom of Information Act (FOIA). We filed an expedited FOIA request on February 1, 2002 seeking records on the development of CAPPS-II. Upon receiving no response from the TSA, we filed a lawsuit on March 15, 2002 to compel the disclosure of relevant

[6] Air Security Focusing on Flier Screening, Washington Post, September 4, 2002.

information.[7] The information that EPIC sought was mostly as Sensitive Security Information (SSI), which is defined as information "the release of which would be detrimental to the safety of passengers in transportation."[8] TSA regulations define SSI to include "any selection criteria used in any security screening process" and "specific details of aviation security measures."[9]

What little information was released gives some sense of the scale of the project being contemplated. A NASA Ames Research Center briefing to Northwest Airlines in December 2001 obtained under the FOIA describes the possible utility of NASA technology for aviation security. The documents outline a vision similar to the "Total Information Awareness" program that is currently being developed by the Defense Department. Biometric identifiers, including face recognition, smart card national identification documents, and extensive data mining of multiple-source transaction records would help give security personnel an indicator that a passenger is a threat or a non-threat.[10] The document acknowledges that a requirement of the proposed passenger screening program would need to "address privacy and 'big brother' issues to the extent possible." While there is no indicator that TSA or Northwest Airlines have engaged NASA to construct CAPPS-II, the NASA proposal provides some limited information about the conceptual underpinning of the CAPPS-II project.

Email records obtained under the FOIA disclose that a CAPPS-II prototype was to be tested at the Salt Lake Winter Olympics in 2002, but was ultimately not deployed due to the legal concerns of the unidentified contractors. Emails obtained under the FOIA also

[7] EPIC v. DOT, Civil Action 02-0475, (D.D.C. 2002).
[8] 49 U.S.C. 40119(b)(1)(C) and 49 CFR 1520.3(b)(3).
[9] 49 CFR 1520.7(c), (j).
[10] NASA Ames Research Center Northwest Airlines Briefing available at http://www.epic.org/privacy/airtravel/foia/foia1.html.

show that the developers of CAPPS-II met with Admiral Poindexter and the Defense Department's Total Information Awareness team to discuss possible collaborative efforts.[11]

A January 29, 2003 contract pre-solicitation notice issued by the TSA about the CAPPS-II system provides more details about the project goals:

> The intent of the CAPPS II program is to improve the ability to identify threats to aviation security by analyzing and evaluating multiple-source data on *every* ticketed passenger on *every* airline to determine whether the passenger poses a security risk or threat to the traveling public.[12] (emphasis added)

The notice indicates that awards for the contract will be issued on February 21, 2003 and that the contractor must be ready to begin work at the Office of National Risk Assessment (ONRA) by February 24, 2003. Perhaps coincidentally, the Privacy Act notice states that the Passenger Database will be housed in the ONRA. This suggests that the Passenger Database might be part of the CAPPS-II initiative.

The contract notice requires potential contractors to describe, among other things, their proficiency in "risk assessment methodologies, including modeling and scoring" and the use of "near neural, Bayesian belief and Perceptual networks," "data management using multiple commercial data providers," and "large data (40 terabytes+) management in near real-time environments." According to newspaper reports, various credit scoring firms and information brokers are vying for these lucrative contracts from the TSA.[13]

A quick sketch of the privacy and security risks of CAPPS-II suggests the significant issues that still require public discussion. First, the risks that commercial data mining methodologies pose when used in more exacting law enforcement situations has

[11] See http://www.epic.org/privacy/profiling/tia/meetingscans.html.
[12] Presolicitation Notice, DTSA20-03-R-00780, published on January 29, 2003.
[13] Air Security Focusing on Flier Screening, Washington Post, September 4, 2002.

not been adequately debated. Fraud management systems rely on capturing deviations from the norm – a challenging task even when tracking a relatively simple problem of credit card fraud. Neural networks at the core of data mining programs rely on a very large number of examples of deviance to "train" the system, it is unclear what examples the TSA will use and whether those examples are reliable indicators of future terrorist action. Even if the system were used to find non-threats, it is not clear what criteria would go into developing a non-threat model and whether the system might operate discriminatorily or punish non-conformity. The tolerance for failure and imprecision in the law enforcement context is significantly different, and the stakes for misidentification are not trivial.

Second, there are also serious questions surrounding law enforcement access to data held by multiple commercial data providers and whether that access might just be an end run around the Privacy Act.[14] EPIC is currently in litigation with the Justice Department to obtain information about its contracts with Choicepoint and other such information brokers to shed light on this question.[15] Additionally, part of the purpose behind the Privacy Act was to ensure that information the government did collect about individuals was accurate.[16] The poor quality of data in the various commercial databases such as credit reports has been well documented.[17] There is a significant possibility that the use of multiple-source commercial databases would result in a number of incorrect determinations because of the bad data stored in these databases – garbage in, garbage

[14] *FBI's Reliance on the Private Sector Has Raised Some Privacy Concerns*, Wall Street Journal, April 13, 2001.
[15] EPIC v. DOJ, C.A. No 02-0063 (CKK) (D.D.C. 2002).
[16] Privacy Act of 1974 Congressional Findings section (b)(4).
[17] See for example, *PIRG: Mistakes Do Happen: Credit Report Errors Mean Consumers Lose*, available at http://www.pirg.org/reports/consumer/ mistakes/. (Finding that over 70% of credit reports have errors, with 30% having serious errors.)

out. Finally, the large database contemplated in the CAPPS-II contract suggests the possible size of the Passenger Database, if indeed it is related to the CAPPS-II initiative.[18] There is no justification or analysis provided for why the government plans to collect and store so much information on individuals.

Driven by similar concerns about the Defense Department's "Total Information Awareness" program, Congress voted to block funding for the initiative unless the Defense Department provided it a detailed analysis of the program and its civil liberties implications.[19] The TSA should provide a similar report concerning the CAPPS-II project. Indeed, the first CAPPS project in 1996 had convened a civil liberties advisory taskforce to provide input into the design of the system. [20]

Or Is the Passenger Database a Watch list or "No-Fly" Database?

Another possibility is that the "risky persons" in the Passenger Database are persons on an official government watch list or "no-fly" list. EPIC has also tried to obtain records about how the TSA is complying with the watch list obligations under the Aviation Transportation Security Act. EPIC filed a request on October 3, 2002 after learning about several reported complaints from members of the public who felt they had been incorrectly placed on a watch list and did not know how to correct the record, or were concerned that they were put on the list for their political opinions. After exhausting all administrative remedies in waiting for a response, EPIC filed suit on December 12, 2002 to compel the disclosure of the information.[21]

---

[18] By comparison, MasterCard's database on 1.7 billion cardholders and all their transactions in a year contain about 40 terabytes of data (without compression). Data Diets, CIO Magazine, January 1, 2003. Available at http://www.cio.com/archive/010103/et_company_content.html.
[19] 108 H.J. Res. 2 (2003).
[20] See http://www.epic.org/privacy/faa/aclu_testimony.html.
[21] http://www.epic.org/privacy/airtravel/tsa_foia_suit.pdf.

TSA has consistently erected barriers to public oversight, which is both a dereliction of duty and a contribution to public confusion about the agency's mission and motives. To date, EPIC has received no documents related to the administration of the watch lists by the TSA, despite the agency being required by law to have such records and to disclose them to the public.

If the TSA is developing the Passenger Database to store "no-fly" or watch list information, then it is not clear why information needs to be collected and stored on all passengers. Any use of watch lists must follow lawful procedures to obtain information about persons on the list and must provide appropriate policy and security safeguards to prevent misuse. Specifically, the TSA should comply with both the letter and the spirit of the Privacy Act of 1974. There also need to be transparent and simple procedures for individuals to challenge determinations. Operators of the watch lists must also be accountable to Congress to ensure that the information is being used appropriately. However, without basic information about how a person is designated a risk and how that might be contested, it is difficult to comment on the use of the Passenger Database as an integrated watch list.

Tracking Individuals' Movements Implicates Constitutional Rights

EPIC submitted comments on February 4, 2003 to the INS on a proposed rule to collect passenger manifest information for all international airline flights.[22] The comments noted that:

> While we believe that the INS has not yet provided adequate information to permit an evaluation of the proposed rule's legality, we note initially

[22] EPIC INS Manifest Comments, February 4, 2003. Available at http://www.epic.org/privacy/airtravel/ins_manifest_comments.pdf.

> that the proposed collection of detailed travel information concerning United States persons clearly raises serious questions under subsection (e)(7) of the Act. The subsection provides that an agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment, unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7) Government collection of information detailing the international travel of United States persons would appear to fun afoul of that prohibition and would, as we discuss below, raise additional constitutional issues.[23]

Similar considerations concerning the Constitutional implications apply to the collection of "PNR and associated data" contemplated by the TSA's notice. While the TSA does at least provide a Privacy Act notice, this notice is not adequate as argued above. We expressly reserve the right to supplement our comments on the Constitutional implications of the Passenger Database after the TSA has provided more information about its proposed information collection.

We note that The Supreme Court has long recognized the right to associate anonymously. *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460 (1958) ("Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly.") *See also Shelton v. Tucker*, 364 U.S. 479, 485 (1960). To the extent that the proposed collection of personally identifying information would enhance the government's ability to track the movements and associations of individuals, it would clearly implicate individuals' right to travel and to associate anonymously.

[23] EPIC INS Manifest Comments, p. 3.

Serious Privacy and Civil Liberty Issues Loom in the Future Direction of TSA

TSA Chief Loy's speech to the National Association of Mayors on January 22, 2003 points to two significant projects that the TSA is currently pursuing, both of which have significant privacy and civil liberties implications that must be more widely debated, particular in Congress.[24] The first is the CAPPS-II project, which Admiral Loy describes as "a system that will allow us to gain much greater comfort with the process by which we select those fewer people to get additional scrutiny before we allow them on an aircraft here in the United States." He described the first goal of the project as taking the system, which the airlines themselves that is currently deal with and manage, out of their hands and bringing the system inside the TSA.

The second goal of CAPPS-II concerns identification. Admiral Loy called for developing "some kind of law enforcement standard for identification" so that the TSA would have "confidence" in a person's identity. The National Research Council has issued a report discussing the significant issues raised by the creation of a national identification document of the sort contemplated by Admiral Loy's comment.[25] The report suggests that, given the scope of the issues raised, any development of such a system must be extensively debated and properly understood by Congress and the public. This element of CAPPS-II has not received such scrutiny to date.

The third goal of CAPPS-II, according to Admiral Loy's speech, is to look for people on the watch list. He said that:

> [CAPPS-II would] bounce that name that we now have some confidence in off an integrated watch list that truly represents foreign terrorists so that

[24] Remarks by Admiral James Loy, U.S. Conference of Mayors, January 22, 2003 available at http://www.tsa.gov/public/display?theme=46&content=486

[25] *IDs-Not That Easy: Questions About Nationwide Identity Systems*. National Research Council, 2002. See also *Your Papers, Please: From the State Drivers License to a National Identification System*, EPIC 2002.

> we can make good judgments as to who in that millions of folks coming to the airport on a daily basis deserves greater scrutiny, as I said before, before they board the aircraft.

This description of CAPPS-II as an integrated watch list is significantly different from the description provided in the contract notice, which states that every passenger's data would be pulled from multiple-source databases and analyzed to see if they pose a risk. The TSA needs to be clear about what precisely it is contemplating, so that the public can have an informed discussion about the privacy and security risks of the CAPPS-II project.

The second project that raises significant privacy and security risks is the "trusted traveler" or "registered traveler" program. This is conceived as a voluntary program where people who are willing to put themselves through a more scrutinized background investigation will gain special "status," which would enable them to receive less scrutiny at airports. This program is a possible precursor to a national ID program, according to the National Research Council, and must be properly understood before any development is to take place.[26] Furthermore, the program presents a significant security risk by creating a hole for potential terrorists, according to former TSA chief John Magaw.[27] Finally, criteria for granting special "status" to some travelers raises significant questions about the equity of the program and whether it would contribute to creating inequality in society.[28]

---

[26] *Id.*.
[27] *Registered Traveler : Program Policy and Implementation Issues*, Government Accounting Office03-253 November 2002 available at http://www.gao.gov/new.items/d03253.pdf.
[28] *Id*.

Conclusion: Questions the TSA Must Answer

The fundamental question about whether this is a Privacy Act notice concerning CAPPS-II, or whether it is a notice concerning watch list information, points to the TSA's singular failure to be publicly accountable and transparent about the information it proposes to collect on individuals. Unless this situation is remedied, it will remain difficult to engage in an informed public debate. We request the TSA to answer the following questions to enable public comments on the merits of their proposal:

1. What is the aim of the Passenger Database? Is it the foundation of CAPPS-II or is it an integrated watch list?
2. What procedure will determine if a person is a "risk"?
3. How does a person become aware of being tagged as a "risk"? And, how can that determination be legally challenged?
4. What specifically are the policy and security safeguards to protect the Passenger Database?

Respectfully submitted,

Chris Hoofnagle
Deputy Counsel

Mihir Kshirsagar
Policy Analyst